Commentary on Directive 2002/58/EC, article3,4 and 5

Poullet, Yves

Published in:
Concise European IT law

Publication date:
2010

Document Version
Publisher's PDF, also known as Version of record

and to cover any message by electronic communications where the simultaneous participation of the sender and the recipient is not required. This concept is thus much broader than that of e-mail. It also includes SMS (Short Message Service), MMS (Multimedia Messaging Service), messages left on answering machines, voice mail service systems including mobile services and 'net send' communications addressed directly to an IP address (Opinion on unsolicited communications, p. 4). Pop-up messages were however not considered by the European Commission as electronic mail (Answer to written question E-3392/02). **(g) Definition of 'personal data breach' (para. 2(h)).** *Purpose*. This definition has been added by the Amending Directive in view of ensuring that citizens are being informed of security failures which could result in their personal data being lost or otherwise compromised. This definition is an essential part of what might be considered as the emerging EU security breach legal framework, which is described more in detail in the comments under art. 4 of the Directive. *Scope*. The terms 'personal data breach' refer to any breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community. Therefore, a data breach is not only existing in cases of unauthorised access to personal data but also in cases of accidental modification or loss of data. The definition covers all breaches occurring in connexion with the provision of communication services, including incidents concerning data processed by an external data processor. Moreover, the breach not only concerns the data which are subject to the communication service but also, and mainly, include data which are processed in the framework of other services provided in connection with the communication service, such as data stored in an electronic mailbox provided together with the internet access service. Finally, the terms 'personal data' are to be construed in the broadest sense – the contrary of the US approach – and include any personal data regardless of the fact that they may not have any economic value or that no economic damages is to be suffered if compromised.

[Services concerned]

Article 3

This Directive shall apply to the processing of personal data in connection with the provision of publicly available electronic communications services in public communications networks in the Community, including public communications networks supporting data collection and identification devices.

1. Scope of the Directive. *Services covered*. The scope of the Directive is defined as follows. It covers all the processing of personal data in connection

with the provision of publicly available electronic communications networks in public communications networks. Therefore, unlike the Old Directive, the scope is not confined to telephony or data networks but also encompasses satellite, terrestrial and cable TV broadcasting networks if of course the identification of the receiver is possible and that without consideration of the type of information conveyed. *Services excluded*. All the processing in connection with electronic communications networks which are not available to the public remain excluded, such as services limited to closed-user groups or services not accessible through public communications networks but for example, through intranet even if these private networks are not limited to closed-user groups like automated teller machines offered in the context of banking services. This exclusion has been criticised by the Working Party who underlined that the distinction between public and private networks will be increasingly difficult to trace and stated the increasing importance of these private networks and the risks associated with their use, for example, by the monitoring of the use of internet by employees within a company (Opinion 2/2008 (150) on the E-Privacy Directive issued May, 15 2008):. If the services offered by companies to customers through their own private networks are certainly excluded from the application of the Directive, they remain subject to the application of the Data Protection Directive's principles. Those principles require inter alia that the processing is lawful, the data processed are relevant and not excessive and the data subjects might exercise their rights to be informed, to access and to rectification. *Extension to RFID networks and the future 'Internet of things'*. The Amending Directive added that the services concerned also include communications services in public communications networks in the Community supporting collection and identification devices. This precision aims at ensuring that public networks used for the transmission of data through Radio Frequency Identification Devices (RFIDs) are also subject to the application of the relevant provisions regarding security, traffic and location data and on confidentiality. RFIDs are considered as a pre-figuration of the 'Internet of things', which constitutes the future of the Internet where physical objects will be connected through a network and provide information about themselves and their surroundings. With the miniaturisation of the terminals to a 'smart dust' and their implantation in objects, clothes or even in human bodies, wireless, sensors and networking technologies, it is now possible to conceive interaction between human beings and their physical environment in new ways. Things might now interact together to send information about themselves and their users through electronic networking to databases. On May 12, 2009, the Commission issued a Recommendation on the implementation of privacy and data protection principles in applications supported by RFIDs (Working Paper on the questions of data protection posed by RFID technology, January 19, 2005, Working Paper 105, asserting a certain number of requirements like 'security and privacy by design', transparency of the RFID applications for the end users, automated deactivation of the chips at the point of sale using RFID tags unless the consumer has opted in for keeping it activated, development of security schemes and obligation for RFID information systems' designers to proceed to a 'Privacy impact assessment' and to make it accessible to the Data Protection Authorities and the end users.

2. Discussion. *Lack of clarity*. The typical services covered by the Directive are not only those offered by the internet access provider, but also all services consisting in the conveyance of electronic signals at the specific request of the recipient of the service but not 'hosting services', content providers' services or 'search engine services', which are indeed 'information society services' and are thereby excluded explicitly by the definition of electronic communication services provided by art. 2(c) of the Framework Directive on electronic communications: 'It (the concept of electronic communications services) does not include information society services as defined in art. 1 of Directive 98/34/EC, which do not consist wholly or mainly in the conveyance of signals on electronic communications networks.' Notwithstanding this clear exclusion, the wording used by the provision creates a certain ambiguity insofar as it refers to services 'in connection with the provision ...' which could broaden, to a certain extent, the material scope of application of the Directive. The ambiguity increases when certain provisions of the Directive are considered that clearly have no meaning if they do not apply to these Information society services or other activities that do not consist 'strictly' in the 'conveyance' of electronic signals, like art. 13 on unsolicited e-mails or art. 5(3) on illegal access to the terminal equipment of a subscriber or user. Nevertheless, most of the provisions only apply to providers or pure electronic communications services, like the provisions on traffic or location data, directories, automatic call forwarding, and so forth. One possible solution is to consider that the material scope of the Directive excludes the processing of personal data in the context of 'activities' that do not consist in providing publicly available electronic communications services on public communication networks, except where the text refers explicitly to other kinds of 'activities' that cannot be identified with the concept mentioned in art. 3(1). Provisions like art. 5(3) on cookies or art. 13 on spamming activities have clearly a broader scope than that defined by art. 3(1).

3. Territorial scope of application. The text refers to services provided 'in the Community'. Some of the services covered by the Directive might be offered to a subscriber or a user inside the European Union from a provider located outside the Community, for example, an internet access service. In that case, the text states clearly that the Directive is applicable. The criterion fixed by the Directive is not the same as the criterion of establishment retained by the Data Protection Directive and will thus permit to a certain extent an extraterritorial effect of this Directive. Notably, the spamming carried out by companies located outside of the Community will be subject to the EU provisions. As regards the services offered by companies operating within the Communities at the moment, it must be underlined that arts. 25

and 26 of the Data Protection Directive will apply in cases of cross-border data flows generated by a service offered by a provider located in the Community. It must be pointed out that it will frequently be the case with internet services insofar as the message is circulating through DNS and root servers located outside the EU. Art. 26(1)(b) of the Data Protection Directive, which provides an exception to the adequate protection when the cross-border data flow, is required for ensuring the performance of the contract between the provider and its customer.

[Security of processing]

Article 4

(1) The provider of a publicly available electronic communications service must take appropriate technical and organisational measures to safeguard security of its services, if necessary in conjunction with the provider of the public communications network with respect to network security. Having regard to the state of the art and the cost of their implementation, these measures shall ensure a level of security appropriate to the risk presented.

(1bis) Without prejudice to Directive 95/46/EC, the measures referred to in paragraph 1 shall at least:

- **ensure that personal data can be accessed only by authorised personnel for legally authorised purposes,**
- **protect personal data stored or transmitted against accidental or unlawful destruction, accidental loss or alteration, and unauthorised or unlawful storage, processing, access or disclosure, and,**
- **ensure the implementation of a security policy with respect to the processing of personal data,**

Relevant national authorities shall be able to audit the measures taken by providers of publicly available electronic communication services and to issue recommendations about best practices concerning the level of security which those measures should achieve.

(2) In case of a particular risk of a breach of the security of the network, the provider of a publicly available electronic communications service must inform the subscribers concerning such risk and, where the risk lies outside the scope of the measures to be taken by the service provider, of any possible remedies, including an indication of the likely costs involved.

(3) In the case of a personal data breach, the provider of publicly available electronic communications services shall, without undue delay, notify the personal data breach to the competent national authority.

When the personal data breach is likely to adversely affect the personal data or privacy of a subscriber or individual, the provider shall also notify the subscriber or individual of the breach without undue delay.

Notification of a personal data breach to a subscriber or individual concerned shall not be required if the provider has demonstrated to the satisfaction of the competent authority that it has implemented appropriate technological protection measures, and that those measures were applied to the data concerned by the security breach. Such technological protection measures shall render the data unintelligible to any person who is not authorised to access it.

Without prejudice to the provider's obligation to notify subscribers and individuals concerned, if the provider has not already notified the subscriber or individual of the personal data breach, the competent national authority, having considered the likely adverse effects of the breach, may require it to do so.

The notification to the subscriber or individual shall at least describe the nature of the personal data breach and the contact points where more information can be obtained, and shall recommend measures to mitigate the possible adverse effects of the personal data breach. The notification to the competent national authority shall, in addition, describe the consequences of, and the measures proposed or taken by the provider to address, the personal data breach.

(4) Subject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which providers are required to notify personal data breaches, the format of such notification and the manner in which the notification is to be made. They shall also be able to audit whether providers have complied with their notification obligations under this paragraph, and shall impose appropriate sanctions in the event of a failure to do so.

Providers shall maintain an inventory of personal data breaches comprising the facts surrounding the breach, its effects and the remedial action taken which shall be sufficient to enable the competent national authorities to verify compliance with the provisions of paragraph 3. The inventory shall only include the information necessary for this purpose.

(5) In order to ensure consistency in implementation of the measures referred to in paragraphs 2, 3 and 4, the Commission may, following consultation with the European Network and Information Security Agency(ENISA), the Working Party on the Protection of Individuals with regard to the Processing of Personal Data established by Article 29 of Directive 95/46/EC and the European Data Protection Supervisor, adopt technical implementing measures concerning the circumstances, format and procedures applicable to the information and notification requirements referred to in this Article. When adopting such measures, the Commission shall involve all relevant stakeholders particularly in order to be informed of the best available technical and economic means of implementation of this Article.

Those measures, designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 14a(2).

1. Obligation to take technical and organisational security measures (para. 1). *Principle.* This article imposes additional security obligations on the provider of a publicly available electronic communications service due to the specificity of the risks linked with the use of the networks. *Concept of 'security'.* The concept of 'security' is quite broad. It means under art. 17(1) of the Data Protection Directive protection 'against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other forms of unlawful processing'. So, for example, the risk of wiretapping by unauthorised third parties during the use of the services requires appropriate safeguards like the use of cryptography or secured lines (e.g. in case of electronic transmission of the credit card number). The possibility of intrusion within the provider's information system in order to collect all its customers' addresses or to manipulate certain data imposes the necessity to install firewalls and other security measures. The sending of worms through the information systems of a communications service provider or the creation of a mirror site in order to lead astray certain communication are other specific risks linked with the use of communications services. The obligation is not limited to technical measures but encompasses also organisational measures which might be the nomination of a data security manager competent to ensure the compliance of the functioning of the service with all Directive provisions. In order to ensure such security, cooperation with the provider of the network might be desirable. Consequently, the operator of the network might be asked to intervene, if an intrusion is detected, to block automatically any access to the information system of the service provider. *Level of security.* The second sentence of para. 1 recalls the criteria developed by art. 17 of the Data Protection Directive to appreciate the level of security to be taken into account by the service provider. Thus, considering the potential risks linked with the nature of the service as regards both the probability of its occurrence and the harm that would result (an electronic communication service in the healthcare sector needs more security measures than a network permitting access to movies), attention will have to be paid both to the state of the art, that is, in particular the standards developed by such standardisation institutes as ISO (on this point, reference might be made to the work of the ISO/IEC/ITU/UN ECE MoU Management Group and Privacy Technology Standards), and to the cost of the implementing the security measures. The more significant the risk, the higher the security level that must be achieved considering the cost of the implementing measures. As regards the kind of measures, emphasis should be placed on the importance of self-regulation in this realm: the development of standards; auditing methods; regimes for the approval of information systems, and so forth. The organisational and technical security of information systems must become an integral part of data protection policy. Finally, recital 20 of the Directive recalls the obligation of the electronic communications service provider to adapt continuously the level of security taking into account the evolution of the state of the art.

2. Additional provisions about the security of processing (para. 1bis). *Justification and content of these measures.* The Amending Directive identifies, without prejudice to Directive 95/46/EC, three measures with respect to security and integrity of networks and communications services that should at least be taken by virtue of para. 1 and which will therefore be mandatory The first one addresses the problem of unauthorised access by employees. Besides the fact that these accesses might be held as criminal infringements, the provision imposes on the providers of publicly available electronic communications services the obligation of developing measures to ensure that personal data can be accessed only by authorised personnel for legally authorised purposes. This may concern systems of identity management in order to effectively fix and control the respective privilege granted to each member of the personnel regarding the access to personal data conveyed, stored or operated by the communications services provider. The second one targets the needed protection of these data against any loss, destruction or illegal access or storage. It refers to various technological security measures, such as the encryption of transmitted data, the adoption of automated control systems about the quality and integrity of stored or transmitted data, the setting up of log in and log out registries, etc. The last security measures mentioned require that the services providers ensure the implementation of a security policy with respect to the processing of personal data. This obligation participates to an increasing accountability of the data controllers by compelling them to envisage the risks associated with the services they provide, to define exactly how they will manage these risks and by making them responsible in case of non respect of their commitments. *Additional competences granted to the national Data protection Authorities.* Besides, para. 1bis attributes two new competences to the Data protection Authorities. The Data protection Authorities must be able – what presupposes for them additional human means – to audit the security measures taken by the providers targeted by the Directive and to issue recommendations about best security practices. This second point has to be underlined since it clearly indicates that the EU authorities favour soft law for regulating the security issues. Art. 16a pleads for an European coordination of these recommendations under the Article 29 Working Party's umbrella.

3. Duty to inform the subscribers (para. 2). *Application.* In addition, the lack of network security and the proliferation of opportunities for illicit actions make it necessary for the providers of electronic communications services to be obligated to issue warnings concerning their use. Art. 4(2) answers this need. In case of 'particular' security risk, for example, the

unexpected appearance of a worm, the discovery of certain failures in the security of its information system or the multiplication of attacks by hackers, the provider of the communications service has the duty to provide information about the existence of these risks and if no action against the risk is available for the service provider, it must alert the subscriber to the possible ways of avoiding the risk including the costs of these remedies, for example, it will advise using certain anti-spam or anti-spyware software. It is quite clear that this provision is applicable to internet access providers who will be requested in case of detection of certain illicit intrusions through their services to implement the appropriate security measures themselves in order to block these intrusions or subsidiary to give to their subscribers the adequate information about the way by which their customers might act against these threats. *Consequence*. The provision suggests that any breach of security will create a sort of 'prima facie' evidence that the service provider is liable if he is unable to demonstrate that he has given the information required or taken the appropriate measures (reversal of the burden of proof).

4. Obligation of provider of publicly available electronic communications services to inform in case of personal data breach (para. 3). *Towards a regulatory framework for security breaches?* As previously noted (see art. 2(h)) the Amending Directive introduces a legal regime for notifying security breaches. The idea comes from the US where in 2003 California passed its 'Data Breach notification Law'. And where at the States' and federal levels, legislative initiatives have been multiplied and have been adopted in more than 40 US states. The EU Commission took the opportunity of the revision of the Directive to introduce the same idea in Europe, even if the scope of the obligations introduced is more limited than in the US legislation. Indeed, the obligation to notify is limited ratione personae to the providers of publicly available electronic communications services and is not applicable to other information services providers like on-line banks or retailers, on-line healthcare or Web 2.0 platforms providers. That restriction has been denunciated by the European Parliament and supported by various actors like the EDPS and the Working Party. So, EDPS asserts: 'I welcome the many improvements in the protection of privacy in the revised e-Privacy Directive. But it is now crucially important to broaden the scope of the security breach provisions to all sectors and further define the procedures for notification'. Notwithstanding these claims for broadening the scope of the security breach provisions, the final compromise maintains the limitation of scope, event if in the same time recital 45b of the Amending Directive states quite clearly that: 'Community law imposes duties on data controllers regarding the processing of personal data, including an obligation to implement appropriate technical and organisational protection measures against, for example, loss of data. The data breach notification requirements contained in Directive 2002/58/EC (Directive on privacy and electronic communications) provide a structure for notifying the competent authorities and individuals concerned when personal data has nevertheless been compromised. Those notification requirements are

limited to security breaches which occur in the electronic communications sector. However, the notification of security breaches reflects a general interest of citizens to be informed about security failures which may result in their personal data being lost or otherwise compromised and about available or advisable precautions that they may take in order to minimise possible economic loss or social harm that could result from such failures. This general interest for users to be notified is clearly not limited to the electronic communications sector and therefore explicit, mandatory notification requirements applicable to all sectors should be introduced at the Community level as a matter of priority [...].' The announcement of a rapid introduction of a global regulation of the security breach not necessarily calls in favour of a legislative action but perhaps for a more flexible self-regulatory environment as will be explained under art. 15, note 6. *Obligation to notify to Data Protection Authorities*. Pursuant to para. 3, the notification is due each time a security breach occurs independently of the seriousness of its consequences. That does not mean that the Data Protection Authorities has to react in any case but the obligation does exist to inform the Data Protection Authorities following a model prescribed by this last one. It is the responsibility of the Data Protection Authorities to develop criteria as regards the selection of cases they will operate on the basis of the notifications received. The notification is due by the provider, according to the terms of the legal provision, 'without undue delay', meaning that a reaction is expected as soon as possible after the discovery of the personal data breaches. *Obligation to notify to subscribers and individuals concerned* The provision inserted by the Amending Directive makes a distinction between the obligation to notify to the Data Protection Authorities which is mandatory in any case and the duty to notify the personal data breach to the subscriber and the persons concerned by the incidents. This duty might indeed benefit of certain exemptions. The reason for these exemptions might be deducted from the main purpose pursued by this obligation. By notifying the incident, subscribers and individual concerned become aware of the risks caused by the fact that their data are compromised and might take, if any, appropriate measures to reduce or to avoid the negative consequences of the security breach. Therefore, if a subscriber learns that his or her code of access has been violated, it will be up to him or to her to modify it immediately. More generally, as explained by the recital 47 of the Amending Directive, a rapid notification will 'allow them to take the necessary precautions'. Furthermore, another reason for providing for exemptions is that the heavy obligation to notify imposed to the provider might be deemed disproportionate, where there is no peculiar risk for the subscriber or other individuals and provided the serious attempt to the provider's reputation which may be incurred by this notification. *Duty of notification – Exemptions*. Therefore, two exemptions have been quite logically enacted. The first one exempts the provider to notify if there is no ground that 'the personal breach is likely to adversely affect the personal data and privacy of a subscriber or an individual'. Even if the concepts remain

vague and will definitively be subject to judicial interpretation for instance, recital 47 of the Amending Directive gives certain examples of what may be considered as being 'adverse effects': it includes not only physical or economic harm but also moral damages like damage to reputation or risks of defamation. The concept is thus broader than in the US's where it only covers the first category of damages. In case of failure of the provider to notify, based on his own judgement about the absence of likely adverse effect, the Data Protection Authority which must be notified may consider that such notification should take place and, pursuant to art. 4(3) third paragraph, require such notification to subscribers and the persons concerned by the incidents. The second exemption relates to the case where the provider has taken preventive technological security measures in order to avoid the likeness of the negative consequences of the security breach or has taken actions in order to render the data unintelligible (and not only less intelligible) for unauthorised persons. The text insists on the fact that these measures need to be effectively implemented and that the exemption is subject to the demonstration of the adequate character of the measures invoked by the provider for justifying the absence of notification. Moreover, the exemption must be approved by the Data Protection Authorities. In light of the above, it might be useful that the provider requests a pre-approval of these measures even if that pre-approval might be subject to certain conditions and to periodic re-evaluation. *Means of providing notification*. Nothing is foreseen under in para. 3 with respect to the way whereby the notification needs to be delivered. General notice in newspapers or, more disputable, through the web site of the provider rather than e-mails sent to each subscriber or individual concerned (which are not necessarily known and identifiable by the provider) seem acceptable. *Content of the notification* What is important is that the notification renders effective the possibility for the latter to react adequately. It means that in certain cases the exact circumstances of the security breach will have to be noticed. The reference to a call centre where additional information about the circumstances of the breach might be provision might also be considered as a less burdensome but still adequate solution for the provider. Now, as regards to the content of the notification, art. 4(3) provides for certain indications. The notification must at least describe, firstly, the nature of the personal breach (i.e., loss of data, identity theft, corruption of data, etc.), secondly, the contact point where information can be obtained and, thirdly, the recommended measures to be taken by the subscribers or the individuals in order to mitigate the negative impact of the incident. It is quite clear that the information provided may not create any confusion and must avoid any ambiguity, for instance by mixing the message about the security breach with advertisement or with an invitation to subscribe to additional services. *Damages*. It is quite clear that, if damages are suffered by subscribers or individuals, a notification made in accordance with para. 3 does not exclude as such the possibility of claiming, by legal proceedings or other ways, for appropriate remedies. In case of regular notification, however, it is the duty

of the notified person to take all reasonable means to mitigate his or her damage and to limit the potential loss.

5. Additional powers conferred to Data Protection Authorities (para. 4). Art. 4(4) grants to the Data Protection Authorities the competence of defining the cases where notification is mandatory, of drawing up standards formats of notification and of determining the manner in which the notification is to be made. Complementary to the competences already assigned by the art. 28(3) of the Data Protection Directive to the Data Protection Authorities, para. 4 foresees the possibility for these Data Protection Authorities to audit the effective compliance by the providers of their obligations of notification. In that context, subpara. 2 imposes on providers to put at the disposal of the Data Protection Authorities an inventory of personal data breaches suffered, their impacts and the remedial actions taken. As stated in recital 45b of the Amending Directive, 'The competent national authorities should have the necessary means to perform their duties, including comprehensive and reliable data about actual security incidents that have led to the personal data of individuals being compromised. They should monitor measures taken and disseminate best practices among providers of publicly available electronic communications services. Providers should therefore maintain an inventory of personal data breaches to enable further analysis and evaluation by the competent national authorities.' Finally, Data Protection Authorities might impose appropriate sanctions if providers fail to take appropriate measures or or to react adequately in case of security breaches.

6. Technical implementing measures through Communications Committee after large consultation (para. 5). The main aim of this paragraph added by the Amending Directive is to ensure consistent implementation of the above mentioned provisions about notifications and security measures through a complex procedure. The Commission – or more precisely, according with the newly adopted art. 14 a of the Directive (see below comments about this article), the Commission assisted by a Committee of Members States representatives chaired by the Commission – is entitled to adopt and enforce common European rules. What seems innovative here is the obligation imposed on the EU Commission to engage, prior to adopting such measures, large consultation with not only the Working Party but also with the EDPS and the European Network and Information Security Agency (the ENISA). Moreover, these measures have to be adopted in accordance with the so called 'with scrutiny' procedure described in the art. 14 a of the Directive which provide that the European Parliament as well as the Council of Ministers can oppose the proposals made by the Commission (see below comments on art. 14).

[Confidentiality of the communications]

Article 5

(1) Member States shall ensure the confidentiality of communications and the related traffic data by means of a public communications network and publicly available electronic communications services, through national legislation. In particular, they shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data by persons other than users, without the consent of the users concerned, except when legally authorised to do so in accordance with Article 15(1). This paragraph shall not prevent technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality.

(2) Paragraph 1 shall not affect any legally authorised recording of communications and the related traffic data when carried out in the course of lawful business practice for the purpose of providing evidence of a commercial transaction or of any other business communication.

(3) Member States shall ensure that the storing of information, or the gaining of access to information already stored in the terminal equipment of a subscriber or user is only allowed on condition that the subscriber or user concerned has given his or her consent, having been provided with clear and comprehensive information in accordance with Directive 95/46/EC, inter alia, about the purposes of the processing. This shall not prevent any technical storage or access for the sole purpose of carrying out the transmission of a communication over an electronic communications network, or as strictly necessary in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service.

1. General: the principle of confidentiality (para. 1). *Secrecy of correspondence*. The principle of the confidentiality of communications has been clearly asserted by the European Court of Human Rights (see *Klass* (ECHR), *Malone* (ECHR), etc.) and derives directly from the art. 8 of the European Convention for the Protection of Human Rights (ECHR) which clearly asserts the secrecy of correspondence and must be interpreted as being applicable irrespective of the technical means used for conveyance (postal card, electronic mail or surfing, etc.). Thus, this principle forbids, as is the case for a postal card, any interference, any interception or surveillance of electronic correspondence. The wording used by the art. 5.1 does suggest a difference between 'communication' and 'traffic data'. *Communication v Traffic Data*. The concept of 'communication' is very wide, as mentioned above. It covers any information exchanged, that is, the content of the message: the e-mail message sent or received; the web page visited; the movie or song sought by the user. This concept is clearly distinguished from the data identifying the communication (sender, receiver, protocol used, etc.) and necessary for conveying the message, that is, following the wording used by the European Directive: the traffic data which are also protected by the same principle according to the ECHR cases. The distinction will, however, permit more exceptions as regards the obligation of confidentiality for traffic data (see art. 6) than for communication (see infra, point 3).

2. Enforcement of the principle (para. 1). 'Members States shall ensure ... through national legislation'. The Directive calls for at least legislative measures in the strict sense to establish the principle and its enforcement means. The adoption of a constitutional principle is not excluded and the legislation to be enacted must comply with the criteria adopted by art. 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms. The second sentence refers to a minimal intervention. 'The Member States shall prohibit listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data, by persons other than users, without the consent of the users concerned, except when legally authorised to do so, in accordance with Article 15(1)'. The text thus refers clearly to the recognition in each Member State of criminal offences related to these infringements in order to prevent third parties from intercepting electronic messages. Therefore, criminal legislation that punishes the classical wiretapping of voice telephony must be extended to all communication means. Other legislative measures might be contemplated, like provisions imposing professional secrecy on all persons in charge of conveying communications or the obligation for all or certain service providers subject to the obligation of confidentiality to be registered according to specific conditions ensuring respect of the condition, for example, nominating an internal audit service, adopting technical or organisational measures in order to prevent any infringements. In conclusion, the States' obligation to ensure confidentiality of communication might be viewed as a complementary duty to the service providers' obligation to implement the appropriate security measures under art. 4 of the Directive discussed above.

3. Exceptions (paras. 1 and 2). *Exception deriving from the scope of the Directive*. The principle as enunciated in the Directive does not cover the communications which are not conveyed by means of a public communications network and publicly available electronic communications services. Therefore, any communication by means of a private network or created in the context of a service not publicly available is not covered by the principle of confidentiality included in this piece of legislation but by the Council of Europe Human Rights Convention and certainly by the Data Protection principles of the Data Protection Directive as the lawfulness and proportionality of the processing, the rights of the subjects of the data and the security principles. The Working Group has broadly criticised this restriction taking into account the same legitimate expectation of privacy existing in the two kind of networks. *Other exceptions explicitly mentioned by the Directive as regards 'communications'*. The Directive provides under art. 5(1) and (2) a

certain number of exceptions to the confidentiality principle as regards communications. Other exceptions are laid down under art. 6 as regards traffic data. First exception: the users themselves might store the message they have received or sent. So it is quite obvious that a user might keep and use e-mail sent or received within the limit of respect of the Data Protection Directive principles as far as they constitute personal data. It must be underlined that this application will require that the collection be operated fairly, which implies, at least, that the subject concerned by these data might have reasonable knowledge of that processing. The second exception is based on the users' consent. Consent is not only required of the user receiving the message but also of the sender, which might be more difficult to obtain. As regards the form of the consent, one might refer to the requirements laid down by the art. 2 of the Data Protection Directive: 'any freely given specific and informed indication of his wishes by which the data subject signifies is agreement to personal data relating to him being processed'. The third exception relates to interceptions by security agencies or law enforcement authorities. It refers to art. 15(1), which will be discussed below. A fourth exception is provided for 'technical storage which is necessary for the conveyance of a communication without prejudice to the principle of confidentiality'. Recital 22 comments extensively on this provision. These activities of 'automatic, intermediate and transient storage' will permit notably storing an e-mail until it is opened by the recipient or developing caching web pages, provided that any personal data related to the users having requested access to the web pages is erased. Art. 5(2) provides a fifth exception when the storage of a communication by a third party is part of a lawful business practice for the purpose of providing evidence of a commercial transaction. Three conditions are imposed to benefit from this exception: the storage must be legally authorised, according to recital 23, both parties to the communication must be informed of the recording and the data stored in this way must be 'erased as soon as possible and in any case at the latest by the end of the period during which the transaction can be lawfully challenged'. As regards concrete application of this exception, cases such as those of specific Healthcare or Banking networks conveying messages of great sensitivity for which traces must be kept might be quoted.

4. Intrusion into the terminal equipment of a subscriber or user (para. 3). *Principle*. Recital 24 does suggest an interesting comparison between the terminal equipment of a user and a private sphere similar to the domicile requiring protection under the European Convention for the Protection of Human Rights and fundamental freedoms. Any intrusion into the electronic domicile through spyware, web bugs, hidden identifiers, like cookies or other similar devices, ought to be considered a violation of the private electronic space (virtual domicile), what could even be viewed as a form of hacking punished by criminal provisions. The provision clearly focuses on protection against intrusion mechanisms independent of the fact that personal data are processed or not through these mechanisms. The provision clearly focuses on protection against intrusion mechanisms irrespective of the fact that personal

data are processed or not through these mechanisms. Recently, a German Constitutional Court decision dated 27 February 2009, addressed the problem of intrusion into the terminal equipment by Law enforcement authorities. In the case at stake, the procedure had been initiated against a Lander's legislation (Northrhine-Westphalia) allowing the secret service to carry out surveillance of suspected persons at distance by introducing spyware in their computers. This intrusion has severely been condemned by the Court which stated a new constitutional right, directly derived from the Dignity and the right to self development enacted by the arts. 1 and 2 of the German Constitution. As expressly asserted by the Constitutional Court, 'the general right of personality (Article 2.1 in conjunction with Article 1.1 of the Basic Law (Grundgesetz – GG)) encompasses the fundamental right to the guarantee of the confidentiality and integrity of information technology systems'. *Forms of intrusion*. Art. 5(3), as modified by the Amending Directive, targets the storing of information and the gaining of access. The first hypothesis refers to cookies placed on the hard disk of the terminal whereas the second one refers to spyware introduced through the network or any other supports connected to the terminal like a CD Rom or a USB key and able to scrutinise the information or software stored in the terminal. *Legitimate use of certain devices*. These intrusions are strictly regulated even if recital 25 of the Directive recognises certain legitimate uses of some of these devices, for instance, cookies installed on a user's hard-disk in order to facilitate the provision of certain services or to verify the user's identity or capacity to conclude certain transactions. It is clearly stated that the use of these mechanisms might be justified on the grounds of legitimate purposes, for example, a session (not a permanent) cookie placed on the terminal equipment during the connection with a website offering travel services in order to be sure that if the connection is interrupted the user does not need to restate all the information already given. Recital 25 points out the fact that 'access to specific website content might be conditional on the well informed acceptance of a cookie or similar device, if it is used for a legitimate purpose'. Therefore, portals that offer access to multiple websites might invoke avoidance of charges as a reason for installing cookies as a condition for offering the services.

5. Conditions for their uses. Certain additional conditions are established by art. 5(3) for allowing the use of such devices. *Duty to inform*. Firstly, it is provided that users be informed clearly and precisely about the purposes of the data generated by the devices introduced into their terminal equipment in such a way to be sure that they are aware of the information being installed. This provision is a clear application of the right to be informed enacted by the Data Protection Directive as expressly asserted by recital 25. It implies that the name of the data controller and the purposes of the processing must also be given. This consequence is important insofar as many tracking devices are introduced by third parties (cyber marketing companies) in the context of invisible hyperlinks between them and the Information Society service called on by the internet user. It should be emphasised that by doing so the Directive

recognises that cookies are personal data, a point that has on occasion been contested in the past. The processing of data generated through these devices is subject to the other principles of the Data Protection Directive. For example, the duration of the placement of a cookie might be limited to the period justified by the legitimate purpose. This consideration is important insofar as, in many cases, cookies are placed for very long periods of time (20-30 years). *Opt-in system.* The most noticeable modification of the art. 5(3) brought by the Amending Directive is the option taken of the European legislator of the opt-in system as claimed by privacy advocates. The activation of this opt-in system ideally presupposes that the internet users' browsers would be configured in such a way to permit the expression of the consent according to the parameters chosen by the users. As EDPS asserts: 'I note in particular the emphasis on more effective enforcement of the rules on spyware and cookies. This has special relevance where privacy rights must be protected in relation to so called targeted advertising.' *Doubts about the scope of this new requirement.* As regards the scope of this modification, certain doubts have been raised. The reference to the conditions regarding the consent introduced by the Amending Directive to para. 3 creates ambiguity because it seems to limit the consent requirement to personal data, as opposed to other types of information. Even if under the opinion of the Working Party about the notion of personal data (Working Paper 4/2007 on the concept of personal data, Working Paper 136 (20 June 2007) as well as of many European national data protection authorities, persistent cookies containing a unique user ID are to be considered as processing personal data and therefore are subject to applicable data protection rules, this position is still contested by certain EU jurisdictions. Anyway, it might still be considered that some cookies (or similar technologies) may not meet the criteria to be qualified as personal data and therefore fall outside the scope of this provision. Second point, as far as the consent requirement is concerned, the provision does not explain how and when obtaining the consent. The provision does not explicitly refer to 'prior' consent. The use of the past tense ('has given') might mean that the European legislator intended to make sure that users are offered a simple opportunity to refuse cookies prior to their installation on users' computers. How will consent have to be obtained in this specific context? The recitals of the Amending Directive include the following remark: 'where it is technically possible and effective, in accordance with the relevant provisions of Directive 95/46/EC, the user's consent to processing may be expressed by using the appropriate settings of a browser or other application'. In its opinion about the Amending Directive, the Working Party strongly objected the idea of using default browser settings as a mean to provide consent. Concerned about the possible erosion of the definition of consent and of a subsequent lack of transparency, the Working Party opined that: most browsers use default settings that do not allow the users to be informed about any tentative storage or access to their terminal equipment. Therefore, default browser settings should be 'privacy friendly' but cannot be a means to collect

free, specific and informed consent of the users, as required in Article 2(h) of the Data Protection Directive. With regard to cookies, the Working Party is of the opinion that the controller of the cookies should inform its users in its privacy statement and may not rely on (default) browser settings'.

6. Exceptions to the opt-in system. Two exceptions to the opt-in system are provided by the Directive. The first one mentions the necessity of 'storage and access for the sole purpose of carrying out or facilitating the transmission of a communication'. Authors believe this exception could allow, for example, a software feature that searches users' address books to obtain e-mail addresses without requesting these from the users themselves. The addresses would then be used for the purpose of sending (unsolicited) e-mails. The second exception expressly mentioned by the last sentence of para. 3 refers to any technical storage or access 'strictly necessary for the provider in order to provide an information society service explicitly requested by the subscriber or user'. The text refers to tracking devices which are strictly necessary and not simply useful, for instance, screen simulator software which renders downloading certain web pages more user-friendly. Furthermore, is it possible to consider that a software seller needs to install 'spyware' within the user's terminal in order to verify whether there is no contra-indication as regards the functioning of the software to be purchased? Under such circumstances, the opt-out solution, consisting in alerting the user to the installation of the device and the reasons why it is desirable, seems more appropriate. It must be added that the Amending Directive limits the benefit of the exception to the direct provider of the service and therefore excludes the possibility for other information services providers to take advantage of the connection opened by the first one to introduce seamlessly cookies or spyware as it might occur with the so-called transclusive hyperlinks.

[Traffic data]

Article 6

(1) Traffic data relating to subscribers and users processed and stored by the provider of a public communications network or publicly available electronic communications service must be erased or made anonymous when it is no longer needed for the purpose of the transmission of a communication without prejudice to paragraphs 2, 3 and 5 of this Article and Article 15(1).

(2) Traffic data necessary for the purposes of subscriber billing and interconnection payments may be processed. Such processing is permissible only up to the end of the period during which the bill may lawfully be challenged or payment pursued.

(3) For the purpose of marketing electronic communications services or for the provision of value added services, the provider of a publicly available electronic communications service may process the data referred